



Center for Educational Performance and Information

www.michigan.gov/cepi

Michigan Education Information System Data Access and Management Policy

The Center for Educational Performance and Information (CEPI) manages the **Michigan Education Information System (MEIS)**, a system designed to collect and store public school data. Through a combination of technology and statewide collaboration, the MEIS supports better policy development and decision-making for improving the performance of Michigan's public schools and students.

The Director of CEPI is the designated authority to establish and maintain a system of data protection for the MEIS in accordance with the Michigan Freedom of Information Act (FOIA), the Privacy Act, and the Family Educational Rights and Privacy Act (FERPA). School districts and other primary providers of the data stored in the MEIS warehouse are the originators and owners of the data. CEPI functions as the custodian of the data. CEPI established this policy to ensure that all data in its custody are securely maintained and to provide safeguards for all personally identifiable information.

Definitions and Background

A *Confidentiality* policy determines how personally identifiable information collected by an authorized agency is protected and delineates when consent for dissemination is required. The Family Educational Rights and Privacy Act of 1974, as amended (FERPA), guards the confidentiality and access to certain educational records. CEPI's Data Access and Management Policy also takes into consideration the Privacy Act of 1974 in order to protect personal records.

To protect the privacy of individual records in the MEIS, a unique number is assigned to each individual's data set. Student records are assigned a Secure Student Identifier (SSI), while educational personnel are assigned a Personnel Identification Code (PIC). Both the SSI and PIC numbers are computer generated and contain no embedded meaning. After being checked for duplicates, they are permanently assigned. Once an identification code has been appended to each individual record, the student's name or the district employee's name and social security number are secured at the highest level. The remaining portion of the individual record, which now contains only the PIC or the UIC, is subject to restricted access defined in this policy and to summative reports.

In addition to establishing a system of unique codes for each individual record, this policy takes advantage of three corresponding private and confidential protections. These include (1) data security, (2) statistical cutoffs, and (3) restricted access.

- 1) **Security** includes the measures put in place by the State of Michigan (SOM) to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. CEPI maintains its data on the Department of Management and Budget's NCR/Teradata warehouse and is compliant with the *Federal Information Technology Security Assessment Framework*. The secure system holds other highly sensitive data such as vital statistics, treasury accounts, and U.S. Internal Revenue Service (IRS), and welfare records. In addition, the MEIS utilizes automatic encryption and secure socket layer during data transmissions making the transfer of data secure as well.
- 2) Statistical cutoffs, as applied by CEPI, help prevent situations where narrowly defined populations produce cells small enough to permit the identification of individuals. The Michigan Freedom of Information Act (FOIA) limits disclosure of private information and states that access shall be provided to the public except for "information of a personal nature if public disclosure of the information would constitute a clearly unwarranted invasion of an individual's privacy," 15.243(1)(a), part 24, of PA 442 of 1976, as amended (FOIA). CEPI utilizes statistical cutoffs when producing summary reports from individual data that relate to groups of students and personnel thus improving confidentiality and privacy.
- 3) **Restricted access** to the data is imposed by CEPI and significantly limits who can view the data and for what purposes. CEPI has created five access levels that are consistent with specific educational purpose as defined in Section 99.2 of FERPA. Those levels are as follows:

Level 1 access allows read/write privileges to all records and fields in the database. This level is permitted for a minimal number of authorized CEPI staff who operate or manage the data warehouse or who are responsible for maintaining the accuracy and security of data, audit checks and corrections to data elements. Access is allowed for select MDE staff for FTE audit related purposes. The staff members are all subject to Michigan's Acceptable Use Policy 1310, Information Standards and Planning.

Level 2 places limits on access to individual records but not on fields within accessible records. Specifically, superintendents (or their designee) of local and intermediate school districts will have read-and-resubmit access to records of their own students and personnel. This allows for validation of data submissions. Superintendents do not have access to information on students or personnel records outside their districts.

Level 3 places limits on fields within records. The most sensitive fields are excluded from access at this level, such as a student's name or an employee's name and social security number. At this level, the PIC and SSI numbers are put into practice. This read-only access level is provided to appropriate CEPI and MDE staff, primarily for the purposes of audits, operations, accreditation, and reporting to state and federal government agencies. Other

professionals may obtain authorization at this level for completing research related to education in Michigan. Research requests will be reviewed on a case-by-case basis using the rules outlined in the *Human Subject Review* application in Appendix A. The specific fields that are available at level 3 can be found in Appendix B.

Level 4 applies to state government agencies other than CEPI and MDE, as well as to state legislators, legislative aides, and other executive branch members. Data on individual students or staff **will not** be accessed by anyone at this read-only level. However, it will be possible to perform limited data mining of the core data sets to produce aggregate reports containing averages or totals that relate to groups of students and professionals. Statistical cutoffs will be utilized at this level if there is a risk that searches will reveal information about individuals in a select group. CEPI will block any aggregate results with a statistical cutoff in which **six or fewer students or educational personnel might be disclosed**.

Level 5 allows read-only access to the general public for viewing standard reports and data tables that are produced and published in aggregated formats on the Web.

Disclosure of Data

A key purpose of the MEIS is to provide access to information that improves the education-related decisions of parents, teachers, administrators, policymakers, and educational stakeholders as well as the general public. Private or confidential data on an individual shall not be created, collected, stored, used, maintained, or disseminated by CEPI in violation of federal or state law and shall not be used for any purpose other than those already stated in the MEIS data dictionaries or by agreement with companies that provide student assessment data. If CEPI enters into a contract with a third party to perform any of CEPI's functions, that agreement shall require that the data be protected in the same fashion. Under this Policy, no private or confidential data will be released except under the following circumstances as stated in Section 99 of FERPA:

1. To individual teachers and officials of the district who have released the data to CEPI when the determination has been made that there are legitimate educational interests;
2. To comply with a subpoena or court order;
3. To honor a request from a judicial order, or an authorized law enforcement unit, or lawfully issued subpoena; (A law enforcement unit refers to all state and local prosecution authorities, all state and local law enforcement agencies, the Department of Corrections, and probation officers who are part of the Judiciary.)
4. To education officials in connection with an audit or evaluation of a federal or state supported education program;
5. To appropriate parties in connection with an emergency if such knowledge is necessary to protect the health and safety of the student or other individuals; (In the case of a health or safety emergency, requests must be directed to the school district that owns the data. The Director may convene a committee to evaluate the request to determine whether the person requesting the information is in a position to deal with the emergency and the extent to which time is of the essence.)

6. To research proposals approved by the Director, when a legitimate educational interest is established.

Data will be released only on the conditions that (1) the party to whom the data are released does not disclose the information to any third party without the prior written consent of the Director, and (2) only when the data are protected in a manner that does not permit the personal identification of an individual by anyone except the party referenced in the disclosure, and (3) the data are destroyed when no longer needed for the purposes under which the disclosure was granted. CEPI will account for all disclosures by retaining the date, nature, and purpose of the disclosure, and to whom the authorized disclosure was made. If CEPI determines that personally identifiable information is improperly disclosed by the initiator of the request or by a third party agent, CEPI will revoke those parties' access privileges to MEIS data for five years. In addition, CEPI will report all violations to the appropriate federal and state enforcement agencies for enforcement the Privacy Act of 1974. The act indicates that parties who disclose individually identifiable information in any manner to any person or agency not entitled to it shall be guilty of a misdemeanor and fined not more than \$5,000.

Destruction of Data

All individual data in the MEIS will be kept for the length of time required by the *Schedule for the Retention and Disposal of Public School Records* (Bulletin #522, Michigan Department of Education, 3/18/97), which is 99 years for data relating to students. Data will be active in the MEIS Warehouse for five years. Longitudinal data shall be archived for 26 years. Data that are no longer needed will be destroyed in a manner that protects the privacy and the confidentiality of the individuals involved.

Requests for Data Access

Upon the written request of any individual under Section 552a(f)(1) of the Privacy Act of 1974 or Section 99.20 of FERPA to gain access to his/her record contained in the MEIS, CEPI will provide it in a comprehensible format and will consider subsequent requests to amend the record if warranted.

CEPI may also receive requests from researchers, education groups, and other parties who express legitimate education interests in the data as stated under Section 99.31(a)(1) of FERPA. The definition of legitimate educational interest can be found in the *Human Subject Review Application*.

There may be times when an interested party wishes to interview or conduct surveys of a unique population and may request access to names and addresses of students. CEPI **cannot** fulfill these requests. Also, when parties request large volumes of data across the five core data sets in the MEIS, the warehouse administrator may review the timing of the request to ensure that processing the request does not degrade the efficiency of the system.

All users of the requested data must sign the *Human Subject Review Application* that explains how the data are to be stored, used, maintained, and disseminated. If permission is granted, the Director of CEPI shall receive a copy of any analysis or reports created with the MEIS data.